

In the Claims

1. (Previously Presented) An apparatus, comprising:
a port;
a storage medium coupled to and accessed by a controller, wherein the storage medium is configured to store an encrypted unique identifier of the apparatus, encrypted identity information of an individual pre-associated with the apparatus, and an encrypted log of unique identifiers of locations the apparatus and the individual have visited;
the controller, coupled to the port, configured to record in the encrypted log on the storage medium, a unique identifier corresponding to a location the apparatus and the individual have visited;
the controller configured to restrict the individual from modifying the encrypted unique identifier of the apparatus, encrypted identity information of the individual pre-associated with the apparatus, and the encrypted log of unique identifiers of locations the apparatus and the individual have visited, as stored in the storage medium; and
the controller, configured to provide, in response to a request from an authorized requestor, one or more of the unique identifier of the apparatus, identity information of the individual pre-associated with the apparatus, and the log of unique identifiers of locations the apparatus and the individual have visited.
2. (Previously Presented) The apparatus of claim 1 wherein the port comprises any one of a firewire port, USB port or an infiniband port.
3. (Previously Presented) The apparatus of claim 1 wherein the storage medium comprises a flash memory.
- 4-9. (Canceled)
10. (Previously Presented) The apparatus of claim 1 wherein the security information can be enhanced or modified by downloading data to the apparatus.

11. (Previously Presented) A system for allowing for secure identification of an individual when accessing information, comprising:

a central hub configured to communicate with a plurality of touchpoints, at least one of the plurality of touchpoints configured to communicate with at least one device, the at least one device comprising:

a port;

a storage medium coupled to and accessed by a controller, wherein the storage medium is configured to store an encrypted unique identifier of the apparatus, encrypted identity information of an individual pre-associated with the apparatus, and an encrypted log of unique identifiers of locations the apparatus and the individual have visited;

the controller, coupled to the port, configured to record in the encrypted log on the storage medium, a unique identifier corresponding to a location the apparatus and the individual have visited;

the controller configured to restrict the individual from modifying the encrypted unique identifier of the apparatus, encrypted identity information of the individual pre-associated with the apparatus, and the encrypted log of unique identifiers of locations the apparatus and the individual have visited, as stored in the storage medium; and

the controller, configured to provide, in response to a request from an authorized requestor, one or more of the unique identifier of the apparatus, identity information of the individual pre-associated with the apparatus, and the log of unique identifiers of locations the apparatus and the individual have visited.

12. (Previously Presented) The system of claim 11 wherein the port comprises any one of a firewire port, USB port or an infiniband port.

13. (Previously Presented) The system of claim 11 wherein at least one of the plurality of touchpoints comprises a personal computer.

14. (Previously Presented) The system of claim 11 wherein the storage medium comprises a flash memory.

15-20. (Canceled)

21. (Previously Presented) The system of claim 11 wherein the security information within the at least one device can be enhanced or modified by downloading data to the at least one device.

22. (Canceled)

23. (Currently Amended) The system of claim 11 wherein the location of at least one of the plurality of touchpoints is selected from the group consisting of: touchpoint comprises any one of an airport, a car rental, a bank, and combinations thereof airports, car rentals, or banks.

24. (Previously Presented) A secure key hub to serve as a centralized data collection point, the hub configured to:

receive and store information from at least one touchpoint regarding usage of a secure key device at the at least one touchpoint, the secure key device comprising a storage medium configured to store an encrypted unique identifier of the secure key device, encrypted identity information of a user of the secure key device, and an encrypted log of identifiers of locations at which the secure key device has been used; and

provide information to the at least one touchpoint to match with information received by the at least one touchpoint from the secure key device in order to identify the user of the secure key device.

25. (New) The secure key hub of claim 24 wherein:

the log of identifiers does not have overwrite capability; and

the at least one touchpoint is to read the log of identifiers and to log touchpoint information within the secure key device regarding usage of the secure key device at the at least one touchpoint.